Autorisations NAS

Autorisations NAS dans OMV7

Général

L'objectif de ce document est de fournir une explication générale des paramètres de contrôle d'accès, à l'aide des partages réseau Samba, dans un réseau peer-to-peer. Il s'agit d'une brève explication des autorisations, telles qu'implémentées dans l'interface graphique () d'Openmediavault , avec quelques exemples utilisables. Elle ne s'applique pas directement aux environnements LDAP ou Domaines. Dans le Guide des nouveaux utilisateurs (https://wiki-omv--extras-org.translate.goog/doku.php?id=omv7:new_user_guide&_x_tr_sl=auto&_x_tr_tl=fr&_x_tr_hl=fr)

d'Openmediavault , dans les sections Configuration d'un dossier partagé (https://wiki-omv--extras-org.translate.goog/doku.php?id=omv7:new_user_guide&_x_tr_sl=auto&_x_tr_tl=fr&_x_tr_hl=fr#setting_up_a_shared_folder) et Création d'un partage réseau SMB/CIF « Samba » (https://wiki-omv--extras-org.translate.goog/

doku.php?
id=omv7:new_user_guide&_x_tr_sl=auto&_x_tr_tl=fr&_x_tr_hl=fr#creating_a_smb_cif_samba_network_share)
, des sélections d'autorisations ont été effectuées qui permettront à **TOUS les utilisateurs** du réseau () local de se connecter aux partages du serveur OMV avec un accès **en écriture** . Pour les administrateurs de réseau () local domestique, avec un ou deux utilisateurs, cela peut être suffisant. D'un autre côté, certains utilisateurs à domicile voudront peut-être empêcher les enfants de supprimer des fichiers et prévoir d'autoriser les connexions d'invités avec un accès en lecture seule. De plus, les petites entreprises peuvent souhaiter accorder ou restreindre l'accès des employés à des actions spécifiques. Ces scénarios nécessiteront que des autorisations soient implémentées pour le contrôle d'accès aux partages NAS. (https://wiki-omv--extras-org.translate.goog/doku.php?
id=omv7:new_user_guide&_x_tr_sl=auto&_x_tr_tl=fr&_x_tr_hl=fr) (https://wiki-omv--extras-org.translate.goog/doku.php?
id=omv7:new_user_guide&_x_tr_sl=auto&_x_tr_tl=fr&_x_tr_hl=fr#setting_up_a_shared_folder)
(https://wiki-omv--extras-org.translate.goog/doku.php?
id=omv7:new_user_guide&_x_tr_sl=auto&_x_tr_tl=fr&_x_tr_hl=fr#creating_a_smb_cif_samba_network_share)
() ()

Une loi immuable pour une bonne sécurité des serveurs

Le mot de passe du compte root (le superutilisateur du serveur) doit être fort et NE doit PAS être partagé. Bien que cela ne soit pas pratique lors de l'exploitation d'un serveur SOHO ou NAS professionnel, le nombre d'utilisateurs connaissant le mot de passe du compte root doit être réduit au minimum. (Dans le cas d'utilisation professionnelle, il doit y avoir au moins deux administrateurs avec un accès root.)

Openmediavault dispose d'un autre compte super utilisateur « **admin** » qui est utilisé pour se connecter à l' interface graphique () d'administration Web . Étant donné que cet utilisateur dispose de capacités « **de type utilisateur root** », le mot de passe de **admin** ne doit pas non plus être partagé.

La raison pour laquelle il est important de contrôler qui a accès aux comptes root et admin ainsi que leurs mots de passe est que ce niveau d'accès peut être utilisé pour remplacer ou contourner toutes les autorisations décrites dans ce document.

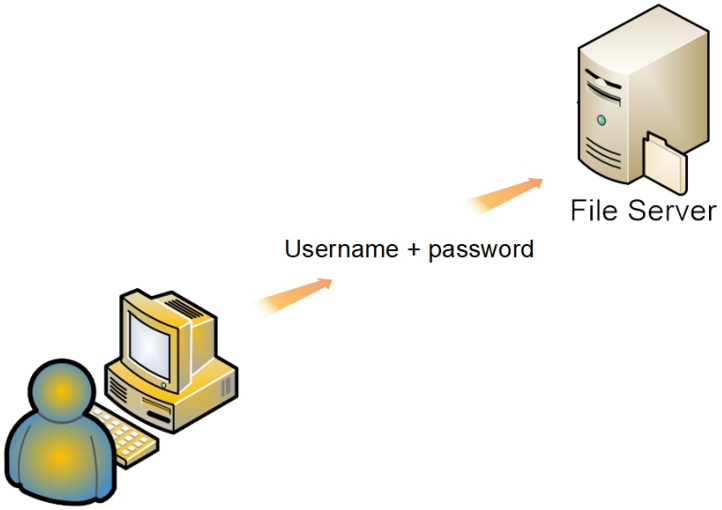
Une connexion au poste de travail

Dans la plupart des environnements LAN () de groupe de travail , les utilisateurs se connectent à leur PC à l'aide d'un nom d'utilisateur et d'un mot de passe uniques. Ces « informations d'identification » sont stockées localement et sont associées à des autorisations qui permettent

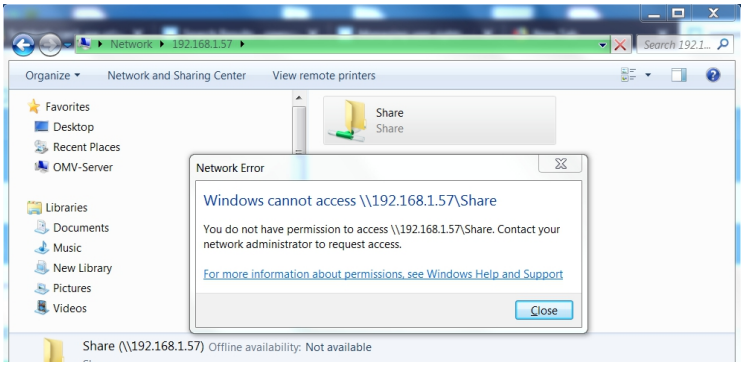
d'accéder au PC local, à ses dossiers et fichiers, ainsi qu'à d'autres ressources du poste de travail. Une recherche de nom d'utilisateur est effectuée, le mot de passe est vérifié et si tous correspondent, l'accès au poste de travail est accordé. Une connexion au serveur « local » est très similaire, permettant l'administration du serveur local.

Accès au partage NAS

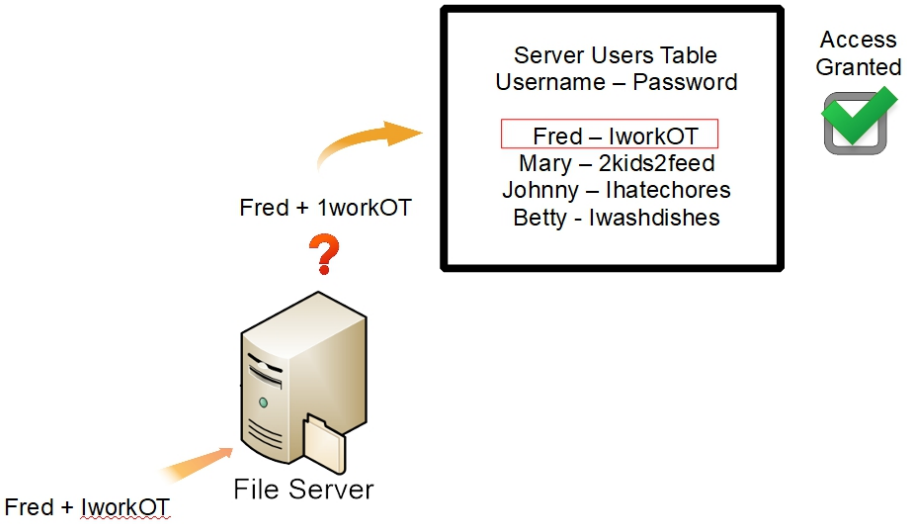
Il en va de même, indirectement, pour l'accès aux partages réseau. Lorsqu'un client LAN () demande l'accès à un partage réseau , un processus d'authentification en arrière-plan est en cours et n'est pas visible pour l'utilisateur. Lorsqu'un utilisateur est connecté à un poste de travail, celui-ci agit comme un « proxy » d'authentification, offrant les informations d'identification de l'utilisateur connecté (**nom d'utilisateur + mot de passe**) au serveur.



Si le processus d'authentification échoue, l'utilisateur peut être invité à fournir d'autres informations d'identification (un autre nom d'utilisateur et un autre mot de passe) ou l'accès est refusé.



Si le processus d'authentification aboutit, l'accès est accordé et le partage est ouvert.



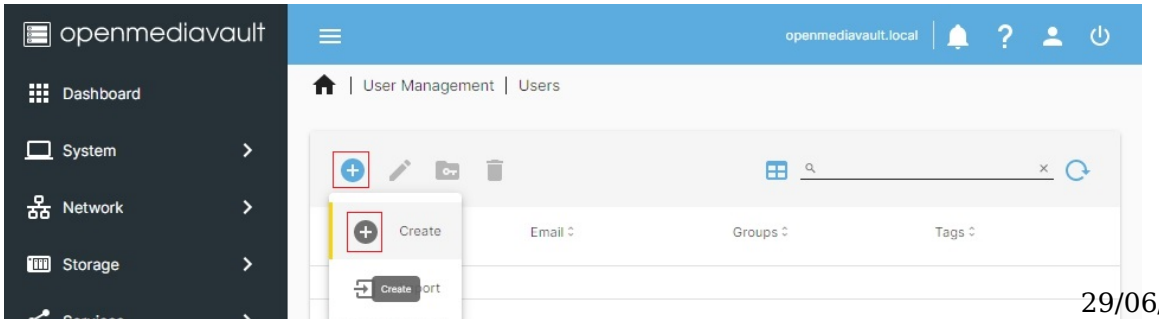
C'est la base pour configurer un accès transparent pour les utilisateurs connectés aux postes de travail lorsqu'ils tentent d'accéder aux partages réseau NAS.

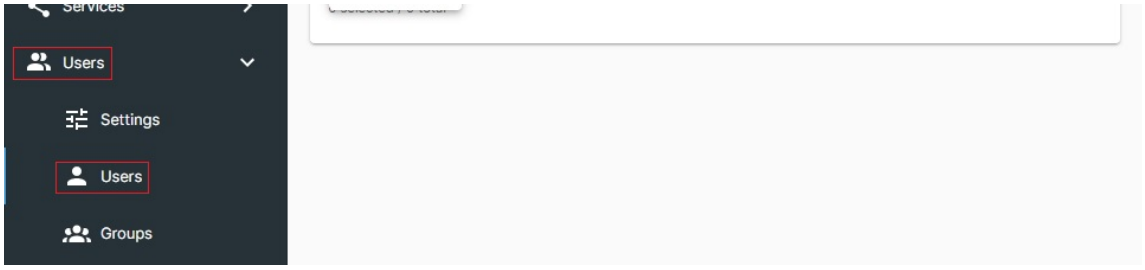
Dans un environnement de groupe de travail, il est relativement facile d'accorder l'accès aux partages par **nom d'utilisateur** et **mot de passe** , mais cela nécessite une certaine configuration. Comme indiqué dans l'exemple ci-dessus, le serveur Openmediavault (ci-après dénommé OMV) doit connaître les noms d'utilisateur et les mots de passe des utilisateurs qui peuvent tenter d'accéder aux partages avec les autorisations activées.

Ajout d'utilisateurs LAN à OMV

Pour permettre un accès transparent, la première étape consiste à ajouter les noms d'utilisateur du poste de travail et leurs mots de passe à OMV.

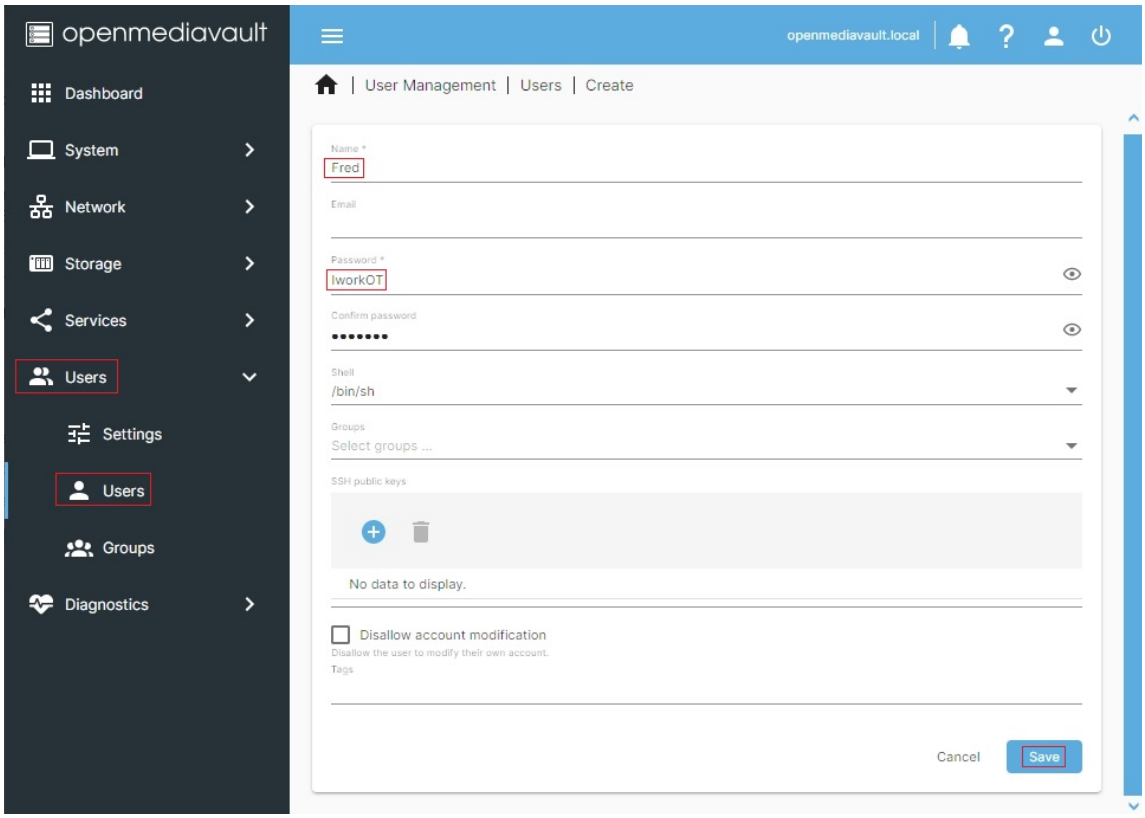
Sous **Utilisateurs** , **Utilisateurs** , cliquez sur le bouton **+Ajouter** . Dans le menu déroulant, cliquez sur **+Créer** .





Nom : Ajoutez le nom d'utilisateur **exactement** tel qu'il est saisi lors de la connexion au poste de travail, avec des lettres majuscules si elles sont utilisées.

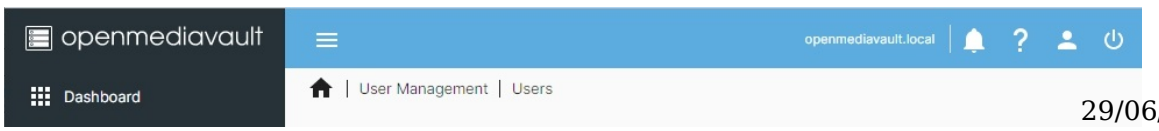
Mot de passe : Ajoutez le mot de passe du nom d'utilisateur exactement tel qu'il est saisi sur le poste de travail. (Dans cet exemple, l'icône en forme d'œil a été utilisée pour afficher le mot de passe démasqué.)

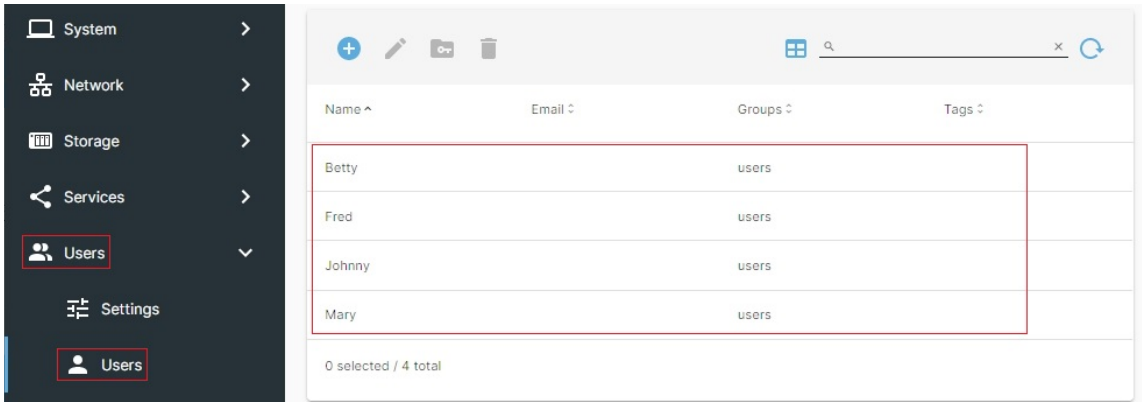


Enregistrez l'entrée et **confirmez** la modification.

Répétez le processus en ajoutant tous les utilisateurs du réseau local () qui auront besoin d'accéder aux partages du serveur où les autorisations sont appliquées.

Le résultat final



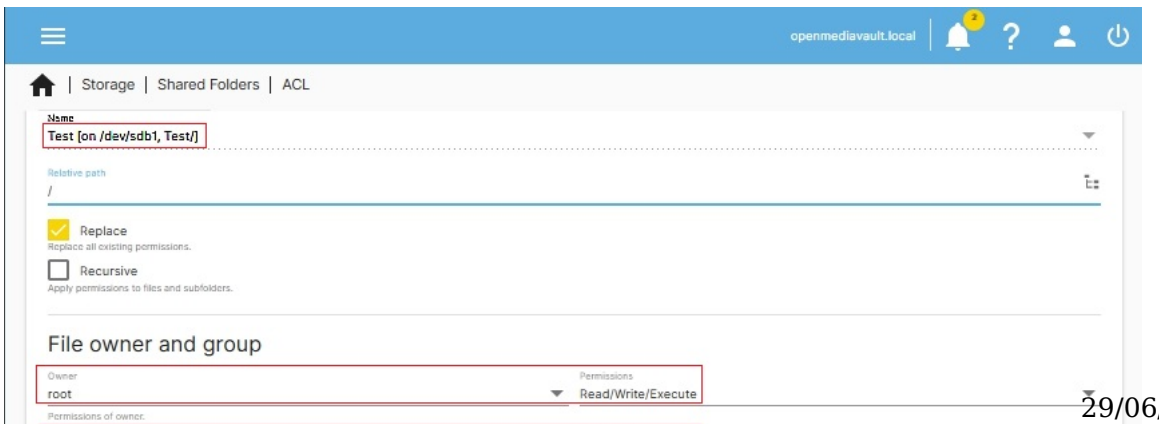


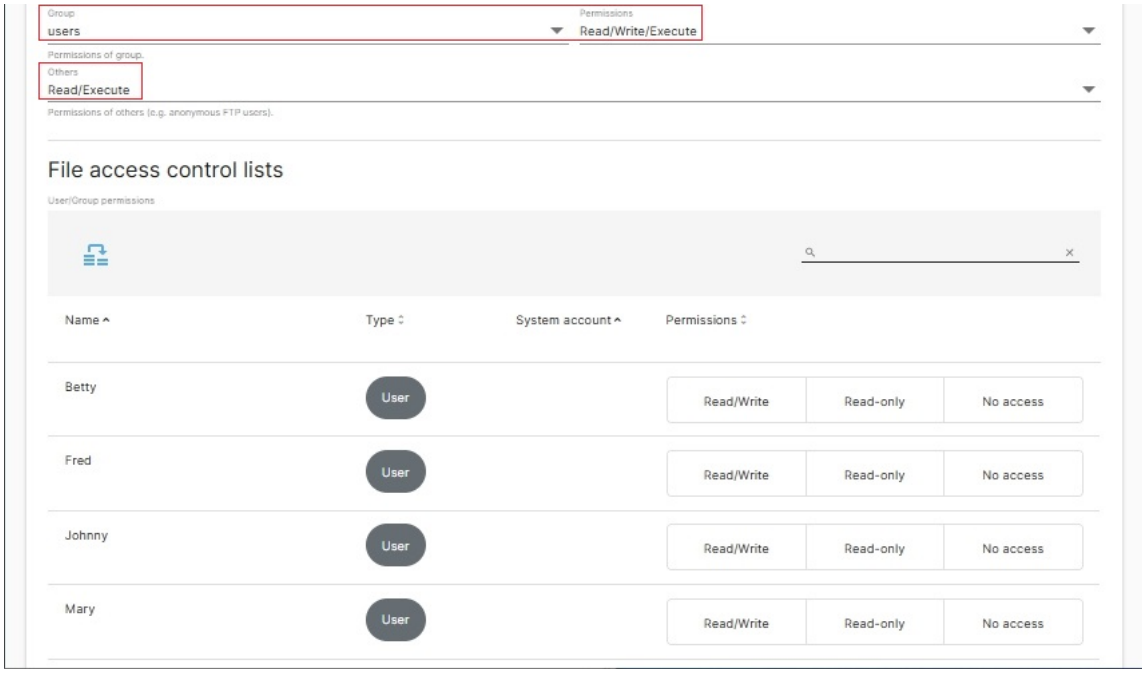
Tous les utilisateurs ont été saisis dans OMV, par le nom d'utilisateur et le mot de passe exacts qu'ils utilisent pour se connecter à leurs postes de travail, ordinateurs portables, etc. Notez que tous les noms d'utilisateur sont dans le groupe **d'utilisateurs** par défaut.

Autorisations des dossiers partagés

Par défaut, la majorité des fichiers et dossiers du serveur de fichiers OMV appartiennent au compte utilisateur **root** et y accèdent . Comme cela n'est pas utile dans un environnement en réseau, l'accès des utilisateurs à un emplacement de stockage du serveur NAS est modifié par la création d'un « **dossier partagé** ». La création d'un dossier partagé est abordée dans le Guide du nouvel utilisateur sous Configuration d'un dossier partagé (https://wiki-omv--extras-org.translate.goog/doku.php?id=omv7:new_user_guide&_x_tr_sl=auto&_x_tr_tl=fr&_x_tr_hl=fr#setting_up_a_shared_folder) . Ce processus crée physiquement le dossier et attribue des autorisations utilisables au dossier, qui autorisent un accès utilisateur régulier. Les autorisations par défaut attribuées à un nouveau dossier partagé, dans l'interface graphique ()

d'OMV , sont (dans ce cas, **Test** est le dossier partagé) : **Administrateur : lecture/écriture/exécution** , **Utilisateurs : lecture/écriture/exécution** , **Autres : lecture/exécution.** Ces autorisations directement correspondre à ce qui suit : ()





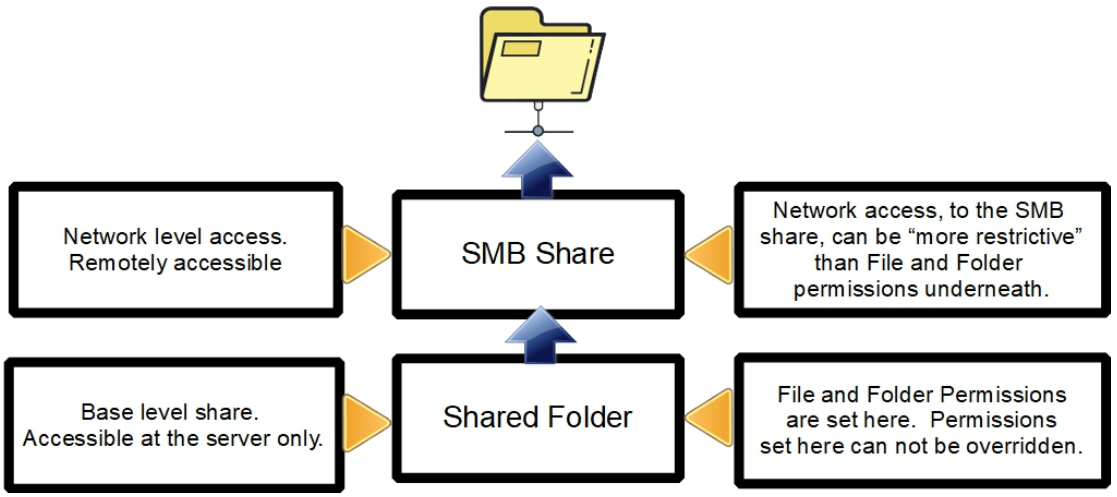
Comme indiqué et illustré précédemment, tous les utilisateurs sont ajoutés par défaut aux **utilisateurs** du groupe. Dans l'exemple fourni ci-dessus, **Fred** , **Mary** , **Johnny** et **Betty** pourront « **Lire, écrire** et **exécuter** » dans le dossier partagé « **Test** ».

Par souci de clarté :

- Le champ intitulé **Fichier, propriétaire et groupe** (ci-dessus) attribue **des autorisations Linux standard** .
- Pour une utilisation sur un serveur domestique et pour simplifier les autorisations du serveur, utilisez uniquement **les autorisations Linux standard** .
- Sous les autorisations Linux standard, « **Autres** » désigne tout utilisateur qui n'est pas **root** ou tout utilisateur qui ne fait PAS partie du groupe **d'utilisateurs** . Cela inclut les membres d'autres groupes et les connexions **anonymes . D'autres** , dans l'exemple ci-dessus, ont **Read**/**Execute** .
- Le champ intitulé **Listes de contrôle d'accès aux fichiers** (ci-dessus) correspond aux **ACL () - (Access Control List)** .
- **NE PAS** mélanger **les ACL avec ()** les **autorisations Linux standard** , sans comprendre les effets ***exacts*** . Lorsque vous utilisez **les autorisations Linux standard** , les cases sous **Listes de contrôle d'accès aux fichiers** ne doivent PAS être cochées.

Partages réseau Samba (SMB)

Bien qu'un **dossier partagé** soit une « base » pour le partage de dossiers et de fichiers, il ne constitue qu'une partie du partage de données sur un réseau. Un dossier partagé permet un accès local , sur le serveur, mais ne permet pas le partage réseau. Le partage réseau nécessite un partage Samba appelé « **SMB**/**CIF » dans** l'interface graphique () d'OMV . (Il existe d'autres techniques de partage réseau, telles que les partages **NFS** , qui ne sont pas couvertes dans ce document.) Comme indiqué dans l'illustration, un partage SMB est superposé à un dossier partagé pour permettre l'accès réseau aux clients LAN . ()



()

Dans ce qui suit; Samba , sous **Services** , **SMB/CIF** , dans l' onglet **Paramètres** est supposé que la case **Activé** est cochée.

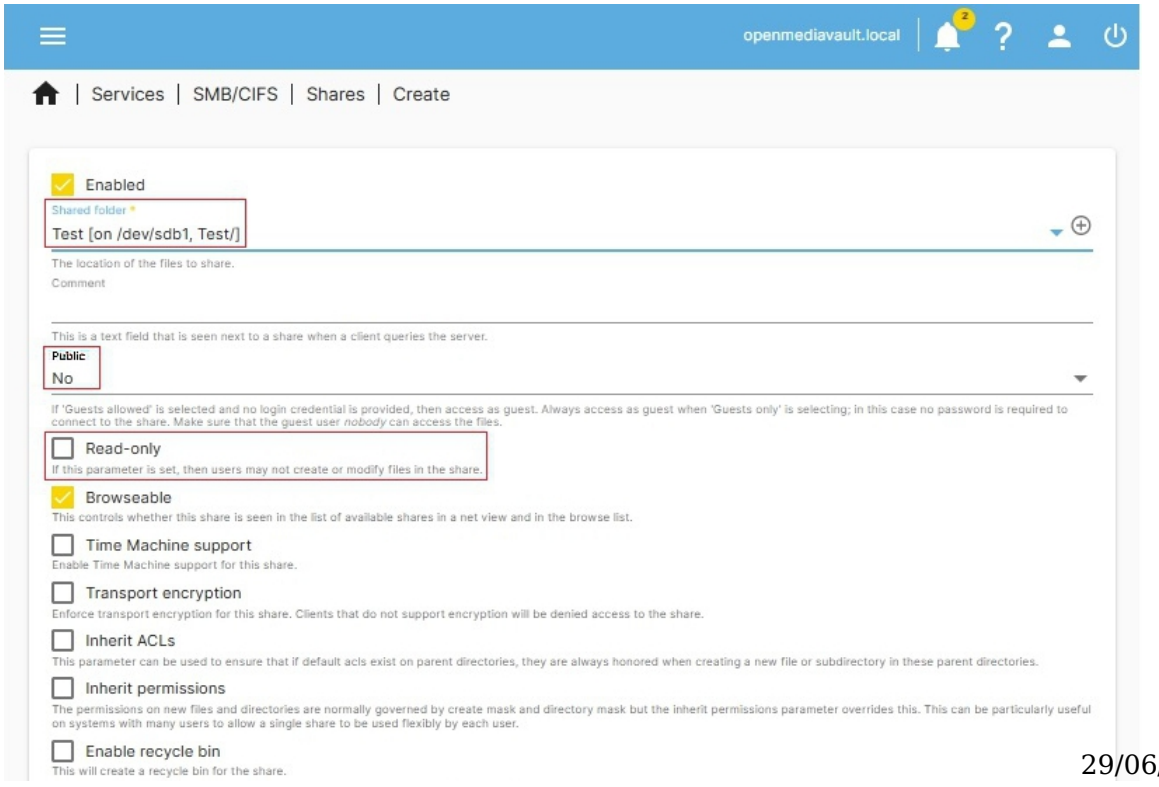
Sous **Services** , **SMB/CIF** , cliquez sur le bouton **Partages** . Cliquez ensuite sur le bouton **+Créer** .

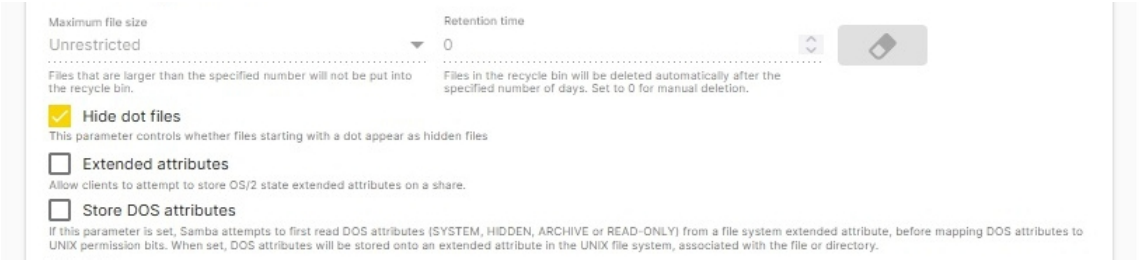
- **Dossier partagé:**

Dans ce cas, nous superposons un partage réseau Samba au-dessus du dossier partagé « Test », créé précédemment.

- **Publique:**

Dans ce cas, l'entrée sélectionnée est **Non** .





- Dans le dossier partagé **de test** , nous avons autorisé l'accès en « **lecture » aux autres** . Le partage réseau SMB (Samba) est superposé au dossier partagé « **Test** ». **D'autres** avec **un accès en lecture** , dans le dossier Partagé, équivaut à « **Invités autorisés** » dans Samba. Cependant, le paramètre SMB « **Public - Non** » arrêtera les utilisateurs anonymes ou inconnus sur le partage réseau. C'est ce que signifiait « Samba peut être plus restrictif » que les autorisations de base sur les dossiers partagés.
- Si le champ **Public** SMB est défini sur « **Invités autorisés** », cela se combinerait avec l'autorisation « **Test** » du dossier partagé **Autres – Lecture** , pour autoriser l'accès **en lecture** aux invités du réseau . (Ces autorisations ; **Autres – Lecture** dans le dossier partagé et **Invités autorisés** dans Samba sont appropriées pour les partages multimédias. Les invités du réseau auraient un accès en lecture aux médias, à la musique, aux films, etc.)
- Au-delà des choix **d'accès public** , Samba suppose que les autorisations utilisateur appropriées ont été attribuées à la couche inférieure, au niveau du dossier partagé.
- Si **Lecture seule** est **activée** (la case est cochée), **les utilisateurs** ayant un accès **en écriture** au dossier partagé ne pourront pas ajouter (écrire), modifier ou supprimer des fichiers dans le partage réseau SMB. (Des exceptions à la règle « Lecture seule » peuvent être faites. Nous y reviendrons plus tard.)

Faites défiler vers le bas de la boîte de dialogue **Ajouter un partage** , à l'aide de la barre de défilement située à droite ou de la touche curseur vers le bas.

Les champs **Hôtes autorisent** 'ed et **Hôtes refusent** 'ed sont des options de contrôle d'accès au niveau du poste de travail . Bien que ces options puissent convenir à certains cas d'utilisation, elles peuvent rendre les autorisations excessivement « compliquées » pour certaines des raisons suivantes.

Il est important de comprendre les effets des autorisations, en particulier la combinaison de divers paramètres. Encore une fois, Samba peut restreindre davantage, mais il ne peut pas outrepasser et « augmenter » l'accès. Certains exemples sont:

- Si un « hôte est autorisé » mais que le nom d'utilisateur n'y a pas accès, le résultat est **refusé** .
- Si un hôte est refusé mais que le nom d'utilisateur y a accès, le résultat est toujours **refusé** .
- Le comportement du routeur consommateur n'est pas toujours cohérent. Si un hôte est spécifié par adresse IP, mais que le client utilise DHCP, l'adresse IP peut changer.
- De nombreux routeurs grand public ne mappent pas systématiquement les noms d'hôte à l'adresse IP, ce qui peut rendre « autoriser » ou « refuser » par nom d'hôte incohérent.

Pour ces raisons et bien d'autres encore, les entrées hôtes ne doivent PAS être utilisées sans examiner attentivement leurs effets.

Options supplémentaires : ce champ présente aux administrateurs de particuliers et de petites entreprises des options intéressantes pour l'administration des partages. Par exemple, dans la moitié supérieure de cette boîte de dialogue Samba, il y a l'option **Lecture seule** . Dans un partage Samba, le **commutateur Lecture seule** restreindra davantage les **utilisateurs** du groupe à un accès **en lecture seule** , même si le dossier partagé ci-dessous autorise l'accès **en écriture** .

Cependant, une « **liste d'écriture** » permettra à un administrateur de contourner sélectivement le commutateur Samba **Read only** . Dans ce cas, si l'instruction `write list=Fred` est ajoutée au champ **Options supplémentaires** , l'utilisateur **Fred** aura un accès **en écriture** tandis que le reste des **utilisateurs** du groupe sera toujours limité à **Read only , appliqué par le commutateur Read only** de Samba .

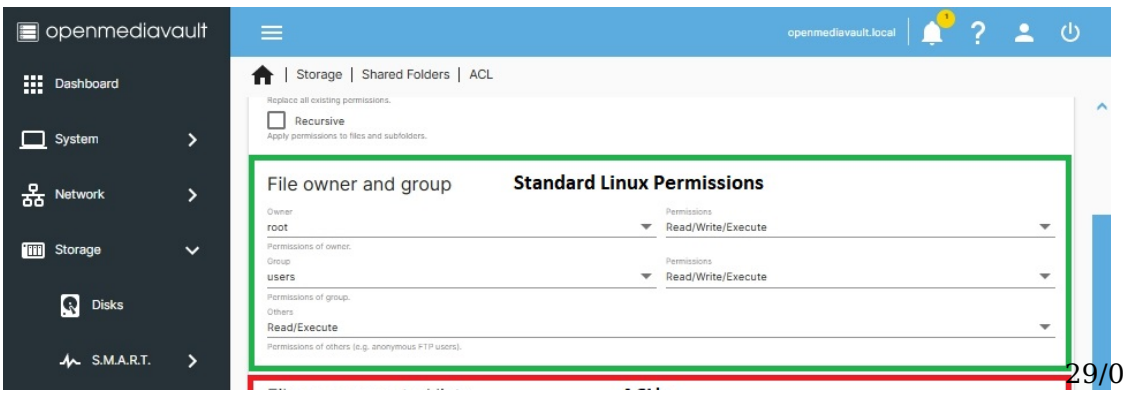
La même chose pourrait être faite pour les **utilisateurs** du groupe avec `write list=@users` l'ajout de cette instruction qui permettrait à l'ensemble des **utilisateurs** du groupe d' accéder **en écriture** tout en restreignant **les autres** avec le **commutateur Lecture seule** .

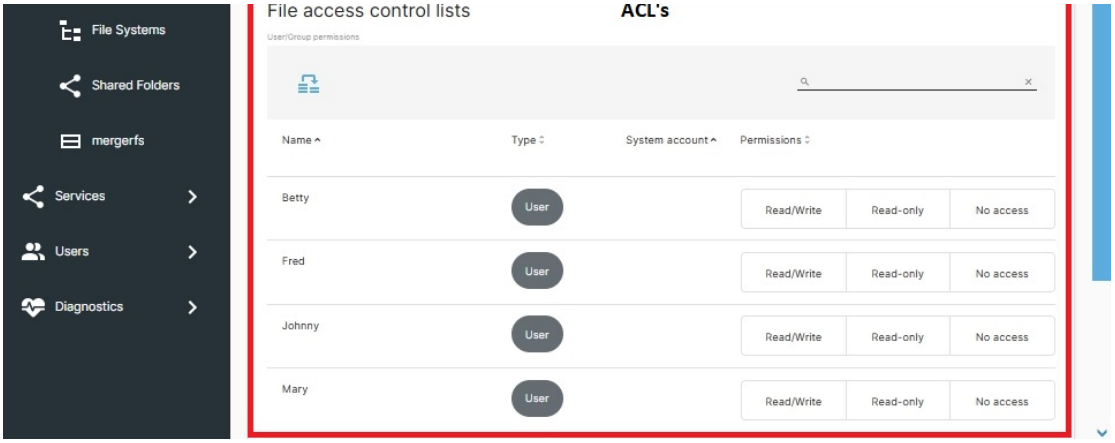
ACL - Autorisations étendues

Général

()Les ACL , () également connues sous le nom **d'autorisations étendues** , ne sont pas natives de Linux. (« Autorisations étendues » ou « ACL » (Access Control List) sont des termes interchangeables.) Les ACL () sont des « modules complémentaires » qui sont stockés avec un fichier ou un dossier dans leurs attributs étendus. L'ACL () accorde ou refuse l'accès aux fichiers/ dossiers en fonction des « noms » d'utilisateur ou de groupe.

Encore une fois, notez ce qui suit :





Dans la mesure du possible, utilisez **les autorisations Linux standard** (étiquetées comme **Propriétaire et groupe de fichiers**).

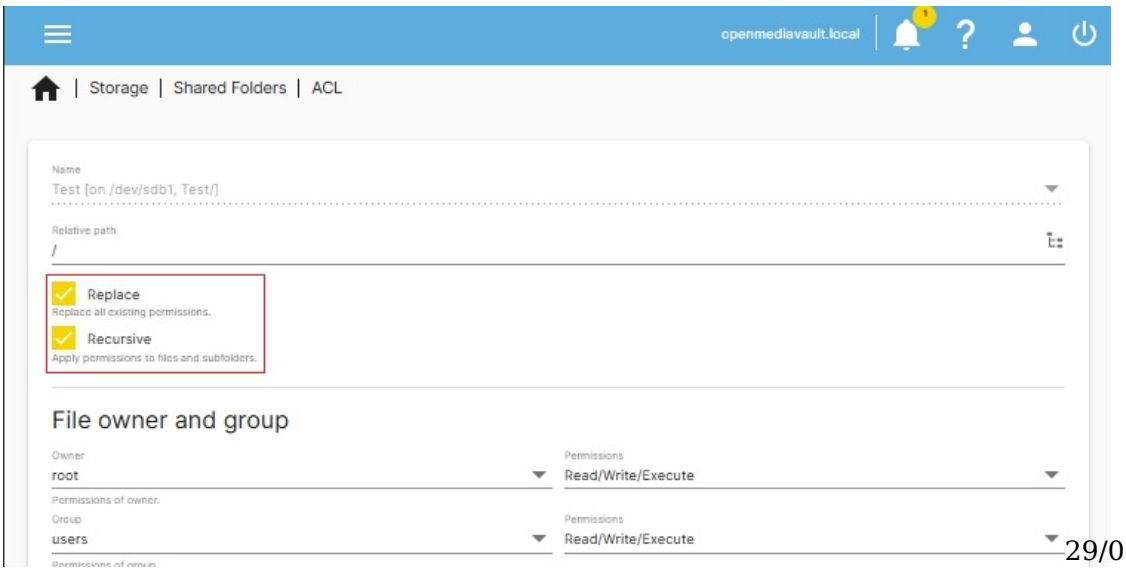
Avertissement

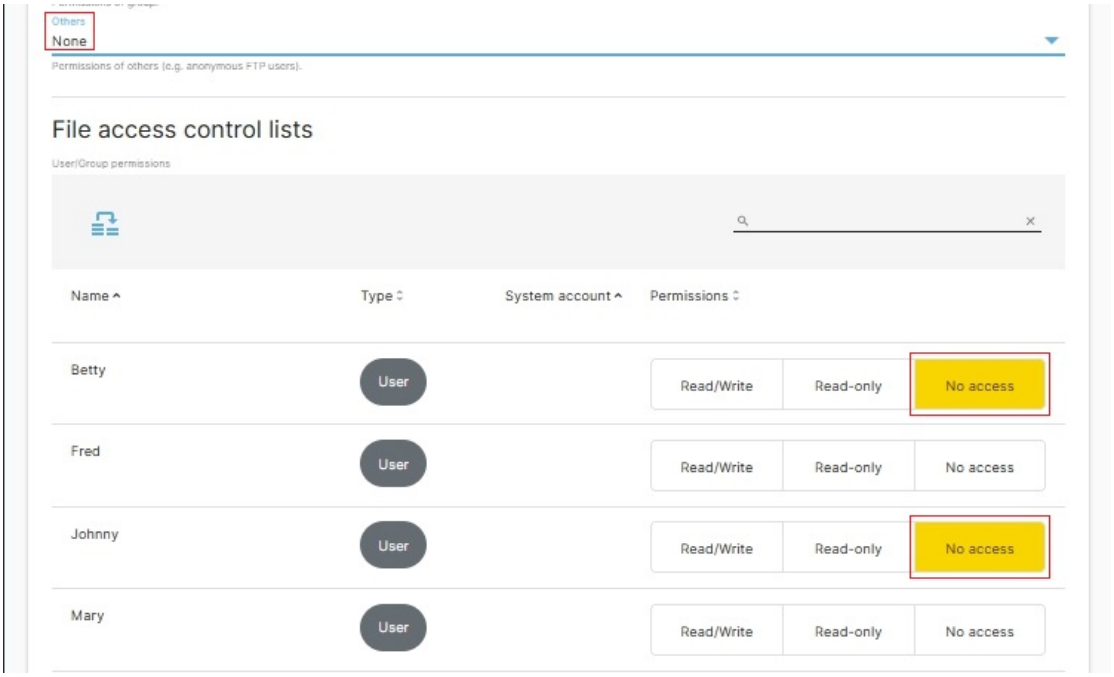
Dans le champ ACL, sous la liste des comptes d'utilisateurs créés par l'administrateur, se trouvent **les comptes système** .
Les comptes système sont des comptes par défaut créés pour les opérations du serveur. Les administrateurs **ne doivent PAS** modifier les autorisations ou les paramètres ACL pour les comptes système. Cela pourrait rendre l'installation du serveur inutilisable.

Dans le cadre d'un NAS Linux, utilisé comme serveur domestique, les **ACL () sont à éviter** . Mélanger les autorisations Linux standard et les ACL () peut provoquer des effets inexplicables, si cela n'est pas fait avec soin. Cependant, les ACL () peuvent être utilisées, si nécessaire, pour « refuser » explicitement l'accès à un ou plusieurs utilisateurs du groupe **d'utilisateurs** .

Par exemple, dans l'exemple **d'utilisateurs** du groupe , nous avons deux adultes **Fred** et **Mary** et leurs deux enfants **Johnny** et **Betty** . Il est facile d'imaginer un scénario dans lequel des adultes pourraient avoir besoin d'un partage réseau auquel leurs enfants ne pourraient pas accéder, contenant des informations médicales, des lettres aux responsables de l'école, etc.

Ce qui suit est une utilisation potentielle des ACL () qui permettrait aux parents d'accéder au partage **Test** de dossier tout en refusant à leurs enfants l'accès au même partage :



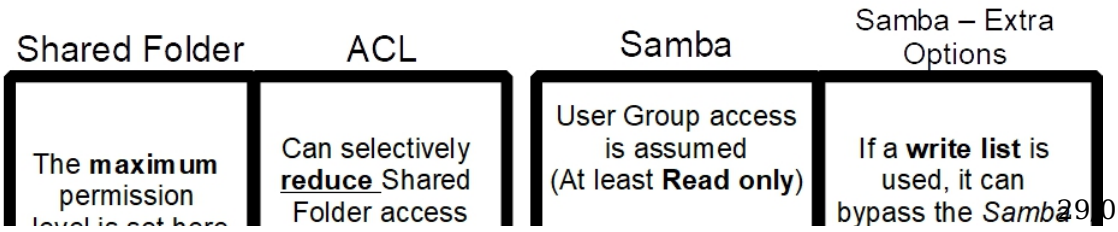


Notez les cases rouges autour de **No access** for **Johnny** and **Betty** . (Pour l'activer, cliquez sur la case. Surligné est activé, clair est désactivé.) Il convient
également de noter que dans un partage privé, « **Autres** » défini sur « **Aucun** » a également du sens.
Pour être sûr que tous les fichiers et dossiers du partage sont réinitialisés avec les autorisations appropriées, les cases **Remplacer** et **Récursif** , en haut, doivent être cochées avant de cliquer sur **Enregistrer** et **Appliquer** .

Après l'enregistrement, **Johnny** et **Betty** n'auront pas accès au partage **Test , tandis que les utilisateurs** restants du groupe auront un accès **en écriture** basé sur les autorisations Linux standard. L'utilisation des ACL () de cette manière permet à un administrateur domestique de définir de manière sélective des utilisateurs individuels, dans le groupe **Users** , sur **Read-only** ou **No access** . Cependant, notez que les ACL ne ()peuvent pas accorder **un accès accru** qui n'existe pas dans les autorisations Linux standard.

Présentation des autorisations

Ce qui suit, de gauche à droite, montre la hiérarchie des autorisations Linux standard et les autorisations réseau qui y sont superposées, avec Samba. Une fois les autorisations standard définies dans le dossier partagé, les couches d'autorisations de suivi ne peuvent que ***réduire*** l'accès. Ils ne peuvent pas, par exemple, accorder à un utilisateur ou à un groupe un accès **en écriture** à un dossier partagé, si **Lecture seule** est spécifié au niveau du dossier partagé.



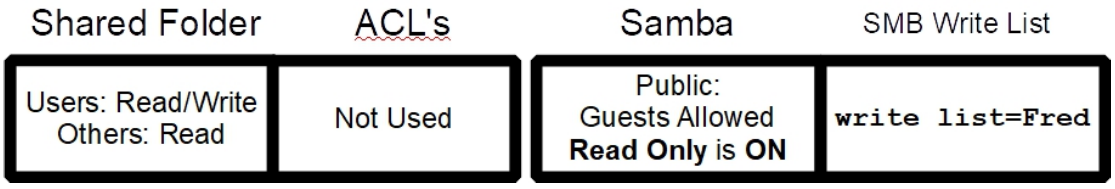
Exemples d'autorisations pratiques

(Dans les exemples suivants, root, en tant que propriétaire, est supposé.)

Dans les exemples, la liste des utilisateurs et leurs mots de passe sont les suivants :
Fred – IworkOT
Mary – 2kids2feed
Johnny – Ihatechore
Betty – Iwashdisches

Tous les utilisateurs sont dans le groupe **d'utilisateurs** par défaut. . Fred est l'administrateur du serveur.

Un partage multimédia



- Dans le dossier partagé, les **utilisateurs** du groupe ont **écrit** . Ceci est nécessaire pour que **Fred** , qui est l'administrateur du serveur familial, puisse **écrire** sur le partage depuis son client.
- L'accès public à Samba est défini sur **Invités autorisés,** ce qui fonctionne avec l'autorisation Dossier partagé **Autres : Lecture** Ces autorisations et paramètres Samba permettront aux visiteurs d'accéder **en lecture** aux partages multimédias tels que la musique ou les films.
- **La lecture seule est activée** . Cela limitera davantage les utilisateurs du groupe de l'accès en **écriture** à **en lecture seule** . Lorsque de jeunes enfants accèdent à un partage, **la lecture seule** est une bonne idée pour éviter la possibilité de suppression accidentelle de fichiers.
- Le Samba `write list` contourne le paramètre Samba **Read Only** pour un utilisateur, permettant à **Fred** d' **écrire** sur le partage à des fins d'administration.

Une part de groupe

(Un emplacement pour partager des fichiers entre tous les membres de la famille ou les membres d'un groupe.)

Shared Folder	ACL's	Samba	SMB Write List
Users: Read/Write Others: Read	Not Used	Public: **NO** **Read Only** is **OFF**	**N/A**

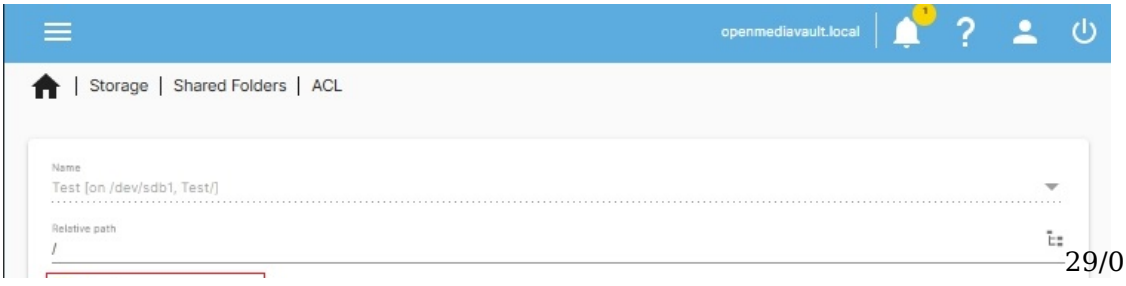
- Les **utilisateurs** du Groupe ont **écrit** .
- Pendant que **d'autres** ont **lu** , dans le dossier partagé, le paramètre **public** SMB est défini sur « **NON** », ce qui arrête tous les utilisateurs qui ne font pas partie du groupe **d'utilisateurs** . Les invités PME ne sont pas autorisés. (Le même effet, aucun utilisateur invité, n'a pu être obtenu au niveau du dossier partagé avec **d'autres – Aucun** .)
- **La lecture seule** est **désactivée** , donc les autorisations du dossier partagé permettent à tous les membres des utilisateurs du groupe d'écrire sur le partage.

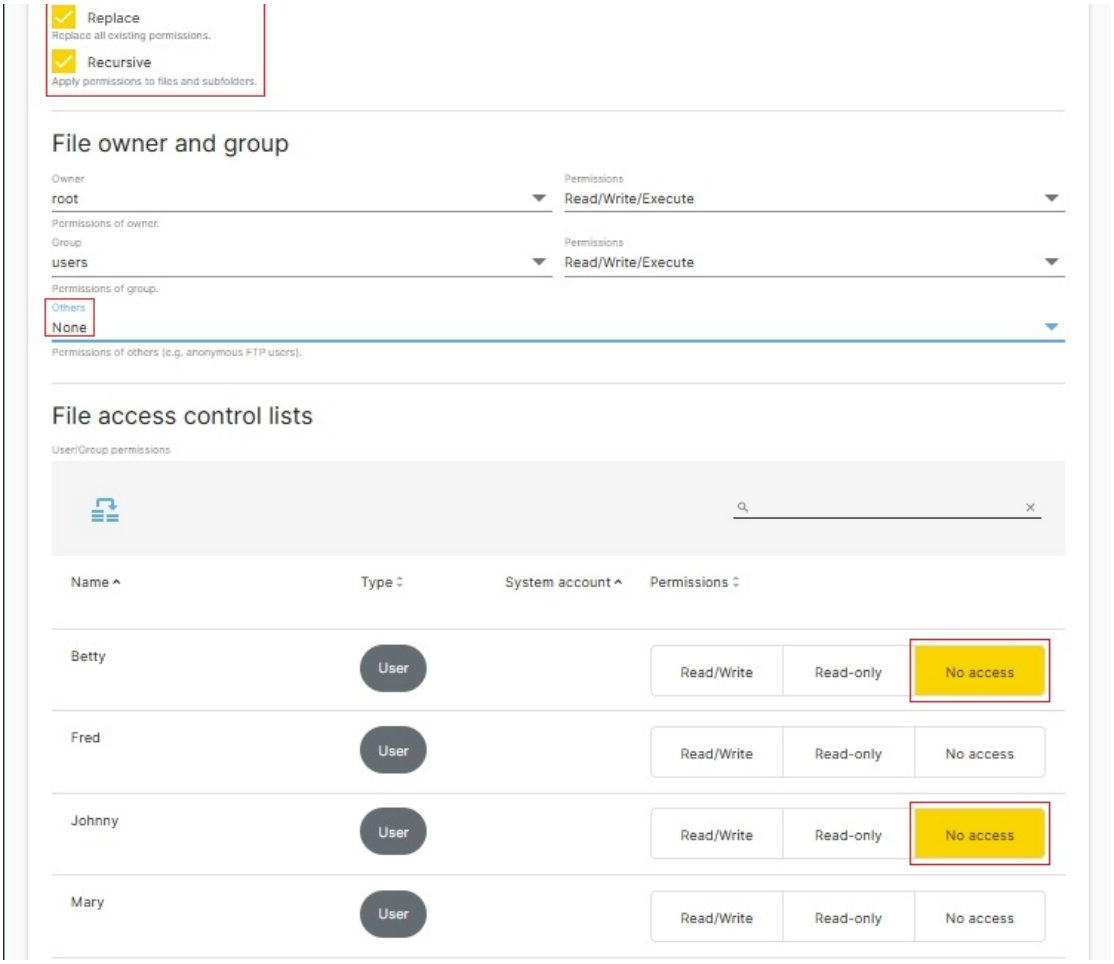
Une action restreinte

Ce partage est destiné à des informations privées, pour certains membres des **utilisateurs** du groupe . Les ACL () peuvent être utilisées pour supprimer l'accès aux utilisateurs qui ne doivent pas voir le contenu du partage applicable. Dans cet exemple, les parents (Fred et Mary) ont accès tandis que les enfants du foyer sont définis sur **No Access** .

Un point important à souligner à propos de cet exemple est qu'un ou plusieurs utilisateurs peuvent être définis en **lecture seule** ou **sans accès** sans perturber l'accès des autres membres du groupe **d'utilisateurs** . Cela peut être pratique et opportun pour les employeurs qui souhaitent restreindre rapidement un employé spécifique à un **accès sans accès** ou à un accès **en lecture seule** , lorsqu'un « avis » a été donné ou reçu. Les paramètres du dossier partagé sont les suivants : Après avoir sélectionné des noms d'utilisateur de groupe spécifiques pour **Aucun accès** (ou **Lecture seule**), il est important de cocher les cases **Remplacer** et **Récursif** avant de cliquer sur le bouton **Enregistrer** . Cela garantit que les nouvelles autorisations sont écrites sur tous les fichiers et dossiers du partage. **Remarque :** ce qui précède peut également être réalisé en créant un nouveau groupe créé sous ; **Accédez à Gestion des Droits** , **Groupe** et cliquez sur le bouton **+Ajouter** . Un groupe nommé **Parents** pourrait contenir les utilisateurs **Fred** et **Mary** . Si le groupe **Parents** est utilisé ci-dessus, dans le champ **Groupe** et avec **Autres** définis sur **Aucun** , les autorisations Linux standard accorderaient l'accès approprié à **Fred** et **Mary** uniquement. Les entrées ACL () pour refuser l'accès aux enfants ne seraient pas nécessaires.

Shared Folder	ACL's	Samba	SMB Write List
Users: Read/Write Others: None	Johnny – No Access Betty – No Access	Public: **NO** **Read Only** is **OFF**	**N/A**



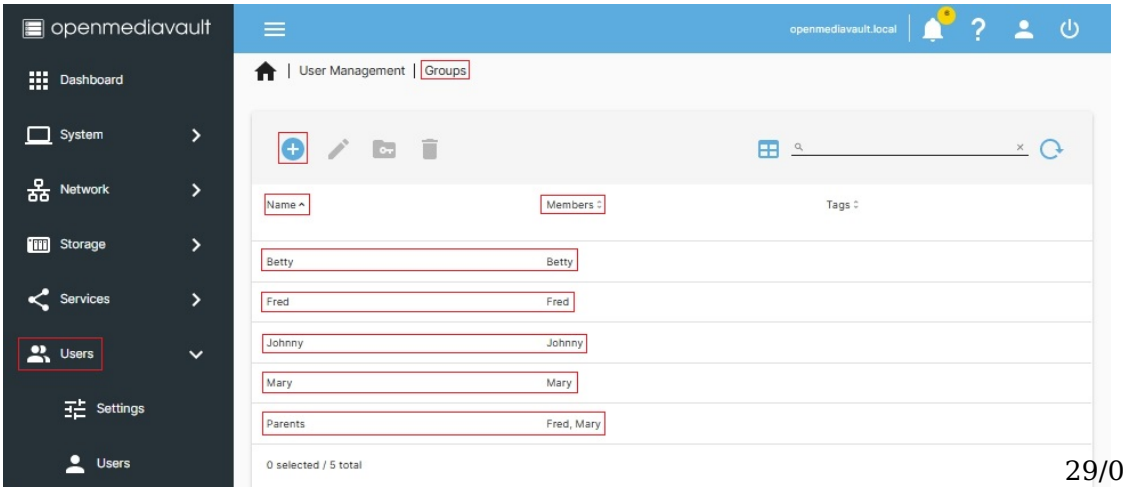


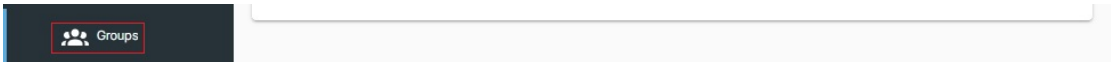
()

Partages personnels/privés

Un partage privé pour un utilisateur individuel peut être créé à l'aide des ACL () et en définissant tous les utilisateurs, sauf un, sur **No access** . Cependant, créer un nouveau groupe avec un utilisateur dans le groupe constitue une meilleure approche.

Notez les noms des groupes nouvellement créés ci-dessous et le nom d'utilisateur dans chaque groupe. Le schéma de dénomination du groupe reste simple.

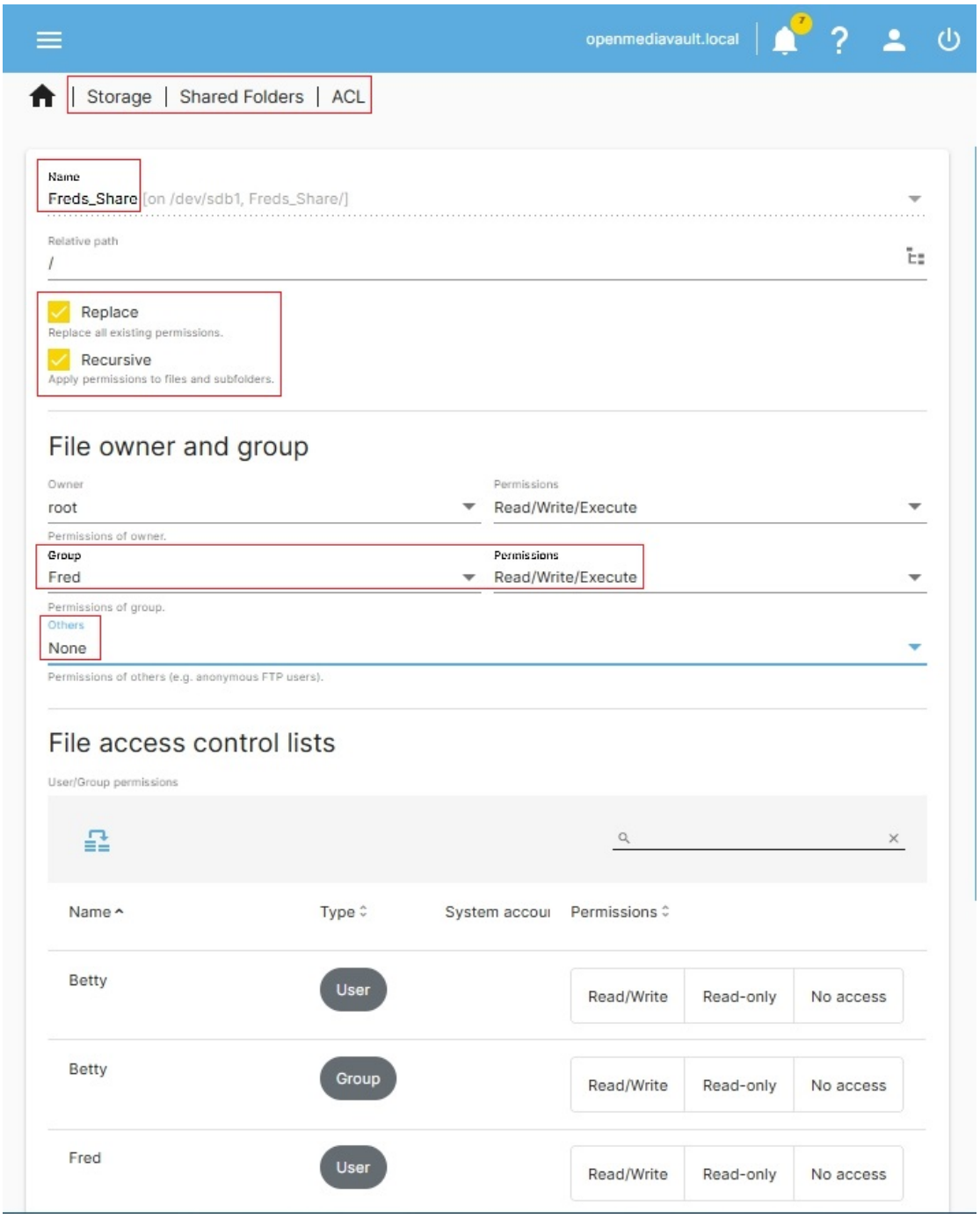




Dans le cas suivant, un dossier partagé a été créé avec le nom **Freds_Share** : Pour définir les autorisations pour un partage privé, les autorisations par défaut du dossier partagé devront être modifiées.

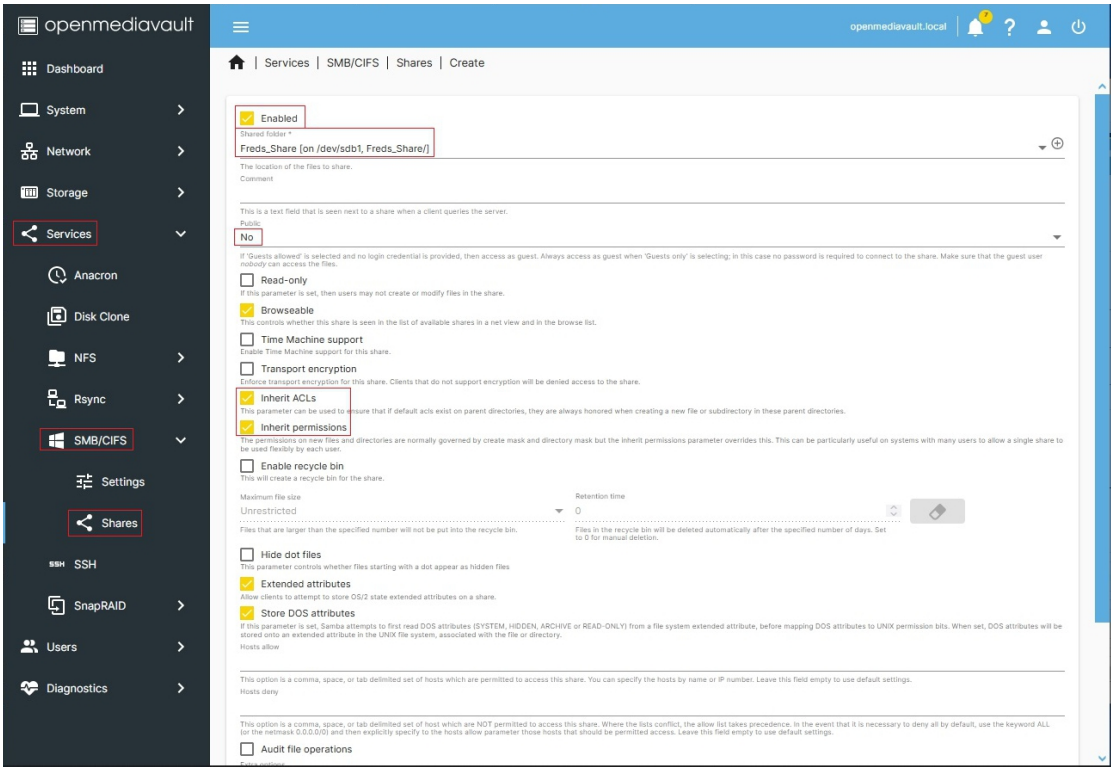
Sous **Stockage** , **Dossiers partagés** , **ACL ()** , mettez en surbrillance **Freds_Share** et cliquez sur le **bouton Liste de contrôle d'accès** .

Dans cet exemple, le groupe **Fred** (avec un seul utilisateur **Fred**) dispose d' un accès **en lecture/écriture/exécution** . Les cases **Remplacer** et **Récursif** sont cochées. **Autres** est défini sur **Aucun** . Ensuite, ces paramètres sont enregistrés. À ce stade, **Fred** est le seul utilisateur pouvant accéder **à Freds_Share** .



Bien que les paramètres du dossier partagé pour **Freds_Share** empêchent toute personne autre

que **Fred** d'accéder au partage, les paramètres SMB indiqués ci-dessous sont en accord avec le dossier partagé de base. Fred sera le seul utilisateur disposant d'un accès en lecture/écriture/exécution à son partage réseau SMB personnel.



En tant qu'examen de Freds_Share, le profil d'autorisations suivant s'applique.

Shared Folder	ACL's	Samba	SMB Write List
Fred: Read/Write Others: None	**N/A**	Public: **NO** **Read Only** is **OFF**	**N/A**

L'essentiel

Si toutes les données sont stockées dans un seul partage, l'attribution des autorisations appropriées peut être difficile, voire impossible. D'un autre côté, si l'on réfléchit soigneusement à la séparation des données en ensembles logiques (dossiers partagés) en gardant à l'esprit l'accès et les autorisations des utilisateurs, l'attribution des autorisations appropriées devient une tâche beaucoup plus facile.

Remarques sur les autorisations :

- Les ajouts de nouveaux utilisateurs ou les modifications apportées aux comptes d'utilisateurs

existants, telles que les changements de mot de passe, devraient être répliqués sur le serveur.
- Certains cas d'utilisation peuvent bénéficier de l'utilisation du Credential Manager (https://translate.google.com/website?sl=auto&tl=fr&hl=fr&u=https://pureinfotech.com/credential-manager-windows-10/) intégré à Win10 et 11.